Quantum Codes from Generalized Reed-Solomon Codes and Matrix-Product Codes

Tao Zhang and Gennian Ge

Abstract

One of the central tasks in quantum error-correction is to construct quantum codes that have good parameters. In this paper, we construct three new classes of quantum MDS codes from classical Hermitian self-orthogonal generalized Reed-Solomon codes. We also present some classes of quantum codes from matrix-product codes. It turns out that many of our quantum codes are new in the sense that the parameters of quantum codes cannot be obtained from all previous constructions.

Index Terms

Quantum MDS codes, generalized Reed-Solomon codes, quantum codes, matrix-product codes, Hermitian construction.

I. Introduction

Quantum error-correcting codes have attracted much attention as schemes that protect quantum states from decoherence during quantum computations and quantum communications. After the pioneering works in [23], [24], the theory of quantum codes has developed rapidly. In [5], [6], Calderbank et. al found a strong connection between a large class of quantum codes which can be seen as an analog of classical group codes, and self-orthogonal codes over $\mathbb{F}_4$. This was then generalized to the nonbinary case in [2], [22]. Recently, many quantum codes have been constructed by classical linear codes with Euclidean or Hermitian self-orthogonality [1], [8], [25].

Let q be a prime power, a q-ary $((n,K,d))$ quantum code is a K-dimensional vector subspace of the Hibert space $(\mathbb{C}^q)^{\bigotimes n} \cong \mathbb{C}^{q^n}$ which can detect up to $d-1$ quantum errors. Let $k = \log_q K$, we use $[[n,k,d]]_q$ to denote a q-ary $((n,K,d))$ quantum code. As in classical coding theory, one of the central tasks in quantum coding theory is to construct quantum codes with good parameters. The following theorem gives a bound on the achievable minimum distance of a quantum code.

Theorem 1.1. ([17], [18] *Quantum Singleton Bound*) *Quantum codes with parameters* $[[n,k,d]]_q$ *satisfy*

$$2d \leq n-k+2.$$

A quantum code achieving this quantum Singleton bound is called a quantum maximum-distance-separable (MDS) code. Just as in the classical linear codes, quantum MDS codes form an important family of quantum codes. Constructing quantum MDS codes has become a central topic for quantum codes in recent years.

As we know, the length of a nontrivial q-ary quantum MDS codes cannot exceed q^2+1 if the classical MDS conjecture holds. The quantum MDS codes of length up to $q+1$ have been constructed for all possible dimensions [11] [12], and many quantum MDS codes of length between $q+1$ and q^2+1 have also been obtained (see [3], [7], [14], [15], [16], [19], [20], [21] and the references therein). However, almost all known q-ary quantum MDS codes have minimum distance less than or equal to $\frac{q}{2}+1$.

In this paper, we construct three classes of quantum MDS codes as follows:

(1) Let q be an odd prime power with the form $2am+1$, then there exists a q-ary $[[\frac{q^2-1}{a}, \frac{q^2-1}{a}-2d+2, d]]$-quantum MDS code, where $2 \leq d \leq (a+1)m+1$.

The research of G. Ge was supported by the National Natural Science Foundation of China under Grant No. 61171198 and Grant No. 11431003, the Importation and Development of High-Caliber Talents Project of Beijing Municipal Institutions, and Zhejiang Provincial Natural Science Foundation of China under Grant No. LZ13A010001.

T. Zhang is with the School of Mathematical Sciences, Capital Normal University, Beijing 100048, China. He is also with the Department of Mathematics, Zhejiang University, Hangzhou 310027, China (e-mail: tzh@zju.edu.cn).

G. Ge is with the School of Mathematical Sciences, Capital Normal University, Beijing 100048, China. He is also with Beijing Center for Mathematics and Information Interdisciplinary Sciences, Beijing, 100048, China (e-mail: gnge@zju.edu.cn).

(2) Let q be an odd prime power with the form $2am-1$, then there exists a q-ary $[[\frac{q^2-1}{2a}-q+1, \frac{q^2-1}{2a}-q-2d+3, d]]$-quantum MDS code, where $2 \le d \le (a+1)m-2$.
(3) Let q be an odd prime power with the form $(2a+1)m-1$, then there exists a q-ary $[[\frac{q^2-1}{2a+1}-q+1, \frac{q^2-1}{2a+1}-q-2d+3, d]]$-quantum MDS code, where $2 \le d \le (a+1)m-1$.

In addition, we also show the existence of q-ary quantum MDS codes with length q^2-1 and minimum distance d for any $2 \le d \le q$, where q is an odd prime power. This result extends those given in [11], [21].

Matrix-product codes were introduced in [4] as a generalization of several well known constructions of longer codes from old ones, for example, the $(a|a+b)$-construction and the $(a+x|b+x|a+b+x)$-construction. In [10], the authors construct some new quantum codes from matrix-product codes and the Euclidean construction. Motivated by this work, we will give a new construction of quantum codes by matrix-product codes and the Hermitian construction. Some of them have better parameters than the quantum codes listed in table online [9].

This paper is organized as follows. In Section II we recall the basics about linear codes, quantum codes and matrix-product codes. In Section III, we give three new classes of quantum MDS codes from generalized Reed-Solomon codes. In Section IV, we present a new construction of quantum codes via matrix-product codes and the Hermitian construction.

II. Preliminaries

Throughout this paper, let $\mathbb{F}_q$ be the finite field with q elements, where q is a prime power. A linear $[n, k]$ code C over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$. The weight wt(x) of a codeword $x \in C$ is the number of nonzero components of x. The distance of two codewords $x, y \in C$ is $d(x, y) = \text{wt}(x-y)$. The minimum distance d of C is the minimum distance between any two distinct codewords of C. An $[n, k, d]$ code is an $[n, k]$ code with the minimum distance d.

Given two vectors $x = (x_0, x_1, \cdots, x_{n-1}),\ y = (y_0, y_1, \cdots, y_{n-1}) \in \mathbb{F}_q^n$, there are two inner products we are interested in. One is the Euclidean inner product which is defined as $\langle x, y\rangle_E = \sum_{i=0}^{n-1} x_i y_i$. When $q = l^2$, where l is a prime power, then we can also consider the Hermitian inner product which is defined by $\langle x, y\rangle_H = \sum_{i=0}^{n-1} x_i y_i^l$. The Euclidean dual code of C is defined as

$$C^{\perp E} = \{x \in \mathbb{F}_q^n | \langle x, y\rangle_E = 0 \text{ for all } y \in C\}.$$

Similarly the Hermitian dual code of C is defined as

$$C^{\perp H} = \{x \in \mathbb{F}_q^n | \langle x, y\rangle_H = 0 \text{ for all } y \in C\}.$$

A linear code C is called Euclidean (Hermitian) self-orthogonal if $C \subseteq C^{\perp E}$ ($C \subseteq C^{\perp H}$, respectively), and C is called Euclidean (Hermitian) dual containing if $C^{\perp E} \subseteq C$ ($C^{\perp H} \subseteq C$, respectively).

For a vector $x = (x_1, \cdots, x_n) \in \mathbb{F}_{q^2}^n$, let $x^q = (x_1^q, \cdots, x_n^q)$. For a subset S of $\mathbb{F}_{q^2}^n$, we define S^q to be the set $\{x^q | x \in S\}$. Then it is easy to see that for a q^2-ary linear code C, we have $C^{\perp H} = (C^q)^{\perp E}$. Therefore, C is Hermitian self-orthogonal if and only if $C \subseteq (C^q)^{\perp E}$, i.e., $C^q \subseteq C^{\perp E}$.

A. Quantum Codes

In this subsection, we recall the basics of quantum codes. Let q be a power of a prime number p. A qubit $|v\rangle$ is a nonzero vector in $\mathbb{C}^q$ which can be represented as $|v\rangle = \sum_{x \in \mathbb{F}_q} c_x |x\rangle$, where $\{|x\rangle | x \in \mathbb{F}_q\}$ is a basis of $\mathbb{C}^q$. For $n \ge 1$, the n-th tensor product $(\mathbb{C}^q)^{\bigotimes n} \cong \mathbb{C}^{q^n}$ has a basis $\{|a_1 \cdots a_n\rangle = |a_1\rangle \bigotimes \cdots \bigotimes |a_n\rangle | (a_1, \cdots, a_n) \in \mathbb{F}_q^n\}$, then an n-qubit is a nonzero vector in $\mathbb{C}^{q^n}$ which can be represented as $|v\rangle = \sum_{a \in \mathbb{F}_q^n} c_a |a\rangle$, where $c_a \in \mathbb{C}$.

Let ζ_p be a primitive p-th root of unity. The quantum errors in q-ary quantum system are linear operators acting on $\mathbb{C}^q$ and can be represented by the set of error bases: $\varepsilon_n = \{T^a R^b | a, b \in \mathbb{F}_q\}$, where $T^a R^b$ is defined by

$$T^a R^b |x\rangle = \zeta_p^{\text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(bx)} |x+a\rangle.$$

The set

$$E_n = \{\zeta_p^l T^a R^b | 0 \le l \le p-1, a = (a_1, \cdots, a_n), b = (b_1, \cdots, b_n) \in \mathbb{F}_q^n\}$$

forms an error group, where $\zeta_p^l T^a R^b$ is defined by

$$\zeta_p^l T^a R^b |x\rangle = \zeta_p^l T^{a_1} R^{b_1} |x_1\rangle \bigotimes \cdots \bigotimes T^{a_n} R^{b_n} |x_n\rangle = \zeta_p^{l+\text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(bx)} |x+a\rangle,$$

for any $|x\rangle = |x_1\rangle \bigotimes \cdots \bigotimes |x_n\rangle$, $x = (x_1, \cdots, x_n) \in \mathbb{F}_q^n$. For an error $e = \zeta_p^l T^a R^b$, its quantum weight is defined by

$$w_Q(e) = \sharp\{1 \leq i \leq n | (a_i, b_i) \neq (0,0)\}.$$

A subspace Q of $\mathbb{C}^{q^n}$ is called a q-ary quantum code with length n. The q-ary quantum code has minimum distance d if and only if it can detect all errors in E_n of quantum weight less than d, but cannot detect some errors of weight d. A q-ary $[[n, k, d]]_q$ quantum code is a q^k-dimensional subspace of $\mathbb{C}^{q^n}$ with minimum distance d. There are many methods to construct quantum codes, and the following theorem is one of the most frequently used construction methods.

Theorem 2.1. ([2] Hermitian Construction) If C is a q^2-ary Hermitian dual-containing $[n, k, d]$ code, then there exists a q-ary $[[n, 2k - n, \geq d]]$-quantum code.

Then we have the following corollary.

Corollary 2.2. *There is a q-ary $[[n, n - 2k, k + 1]]$ quantum MDS code whenever there exists a q^2-ary classical Hermitian self-orthogonal $[n, k, n - k + 1]$-MDS code.*

B. Matrix-Product Codes

In this subsection, we review some notations and results of matrix-product codes. Let $C_1, C_2, \cdots, C_s$ be a family of s codes of length m over $\mathbb{F}_q$ and $A = (a_{ij})$ be an $s \times l$ matrix with entries in $\mathbb{F}_q$. Then, the matrix-product code $[C_1, C_2, \cdots, C_s] \cdot A$ is defined as the code over $\mathbb{F}_q$ of length ml with generator matrix

$$\begin{pmatrix} a_{11}G_1 & a_{12}G_1 & \cdots & a_{1l}G_1 \\ a_{21}G_2 & a_{22}G_2 & \cdots & a_{2l}G_2 \\ \vdots & \vdots & \cdots & \vdots \\ a_{s1}G_s & a_{s2}G_s & \cdots & a_{sl}G_s \end{pmatrix},$$

where $G_i,\ 1 \leq i \leq s$, is a generator matrix for the code C_i. The following theorem gives a characterization of matrix-product codes.

Theorem 2.3. [13], [10] The matrix-product code $[C_1, C_2, \cdots, C_s] \cdot A$ given by a sequence of $[m, k_i, d_i]$ linear codes C_i over $\mathbb{F}_q$ and a full-rank $s \times l$ matrix A is a linear code whose length is ml, it has dimension $\sum_{i=1}^{s} k_i$ and minimum distance larger than or equal to $\delta = \min_{1 \leq i \leq s}\{d_i \delta_i\}$, where δ_i is the minimum distance of the code on $\mathbb{F}_q^l$ generated by the first i rows of the matrix A.

In order to construct quantum codes from matrix-product codes, we need the following theorem.

Theorem 2.4. [4] Assume that $C_1, C_2, \cdots, C_s$ are a family of linear codes of length m and A is a nonsingular $s \times s$ matrix, then the following equality of codes happens

$$([C_1, C_2, \cdots, C_s] \cdot A)^\perp = [C_1^\perp, C_2^\perp, \cdots, C_s^\perp] \cdot (A^{-1})^t,$$

where B^t denotes the transpose of the matrix B.

III. New Quantum MDS Codes from Generalized Reed-Solomon Codes

We first recall the basics of generalized Reed-Solomon codes. Choose n distinct elements $a_1, \cdots, a_n$ of $\mathbb{F}_q$ and n nonzero elements $v_1, \cdots, v_n$ of $\mathbb{F}_q$. For $1 \leq k \leq n$, we define the code

$$\mathrm{GRS}_k(\mathbf{a}, \mathbf{v}) := \{(v_1 f(a_1), \cdots, v_n f(a_n)) | f(x) \in \mathbb{F}_q[x] \text{ and } \deg(f(x)) < k\},$$

where $\mathbf{a}$ and $\mathbf{v}$ denote the vectors $(a_1, \cdots, a_n)$ and $(v_1, \cdots, v_n)$, respectively. The code $\mathrm{GRS}_k(\mathbf{a}, \mathbf{v})$ is called a generalized Reed-Solomon code over $\mathbb{F}_q$. It is well known that a generalized Reed-Solomon code $\mathrm{GRS}_k(\mathbf{a}, \mathbf{v})$ is an MDS code with parameters $[n, k, n-k+1]$. The following lemma presents a criterion to determine whether or not a generalized Reed-Solomon code is Hermian self-orthogonal. We assume that $0^0 := 1$.

Lemma 3.1. *Let* $\mathbf{a}=(a_1,\cdots,a_n)\in\mathbb{F}_{q^2}^n$ *and* $\mathbf{v}=(v_1,\cdots,v_n)\in(\mathbb{F}_{q^2}^*)^n$*, then* $\mathrm{GRS}_k(\mathbf{a},\mathbf{v})\subseteq\mathrm{GRS}_k(\mathbf{a},\mathbf{v})^{\perp H}$ *if and only if* $\sum_{i=1}^n v_i^{q+1}a_i^{qj+l}=0$ *for all* $0\le j,l\le k-1$*.*

Proof: Note that $\mathrm{GRS}_k(\mathbf{a},\mathbf{v})\subseteq\mathrm{GRS}_k(\mathbf{a},\mathbf{v})^{\perp H}$ if and only if $\mathrm{GRS}_k(\mathbf{a},\mathbf{v})^q\subseteq\mathrm{GRS}_k(\mathbf{a},\mathbf{v})^{\perp E}$. It is obvious that $\mathrm{GRS}_k(\mathbf{a},\mathbf{v})^q$ has a basis $\{(v_1^qa_1^{iq},\cdots,v_n^qa_n^{iq})|0\le i\le k-1\}$, and $\mathrm{GRS}_k(\mathbf{a},\mathbf{v})$ has a basis $\{(v_1a_1^i,\cdots,v_na_n^i)|0\le i\le k-1\}$. So $\mathrm{GRS}_k(\mathbf{a},\mathbf{v})^q\subseteq\mathrm{GRS}_k(\mathbf{a},\mathbf{v})^{\perp E}$ if and only if $\sum_{i=1}^n v_i^{q+1}a_i^{qj+l}=0$ for all $0\le j,l\le k-1$. ■

Now we consider generalized Reed-Solomon codes over $\mathbb{F}_{q^2}$ to construct quantum codes.

A. New Quantum MDS Codes of Length $\frac{q^2-1}{a}$

Theorem 3.2. *Let* q *be an odd prime with the form* $2am+1$*,* ω *be a fixed primitive element of* $\mathbb{F}_{q^2}$ *and* $n=\frac{q^2-1}{a}$*. Suppose* $\mathbf{a}=(\omega^a,\omega^{2a},\cdots,\omega^{na})\in\mathbb{F}_{q^2}^n$*,* $\mathbf{v}=(\omega^{q-1},\omega^{q-1},\omega^a,\omega^a,\cdots,\omega^{q-1-a},\omega^{q-1-a},\cdots,\omega^{q-1},\omega^{q-1},\omega^a,\omega^a,\cdots,\omega^{q-1-a},\omega^{q-1-a})\in\mathbb{F}_{q^2}^n$ *and* $1\le k\le(a+1)m$*. Then* $\mathrm{GRS}_k(\mathbf{a},\mathbf{v})\subseteq\mathrm{GRS}_k(\mathbf{a},\mathbf{v})^{\perp H}$*.*

Proof: For $0\le j,l\le k-1\le(a+1)m-1$, we have

$$\begin{aligned}&\sum_{i=1}^n v_i^{q+1}a_i^{qj+l}\\&=\sum_{i=1}^{\frac{q-1}{a}}\omega^{ai(q+1)}\sum_{s=0}^{\frac{q-1}{2}}(\omega^{[2s(q-1)+a(2i+1)](qj+l)}+\omega^{[2s(q-1)+a(2i+2)](qj+l)})\\&=\sum_{i=1}^{\frac{q-1}{a}}\omega^{ai(q+1)}(\omega^{a(2i+1)(qj+l)}+\omega^{a(2i+2)(qj+l)})\sum_{s=0}^{\frac{q-1}{2}}\omega^{2s(q-1)(qj+l)}.\end{aligned}$$

Note that

$$\sum_{s=0}^{\frac{q-1}{2}}\omega^{2s(q-1)(qj+l)}=\begin{cases}0; & \text{if } \frac{q+1}{2}\nmid(qj+l),\\ \frac{q+1}{2}; & \text{if } \frac{q+1}{2}|(qj+l).\end{cases}$$

Now assume that $qj+l=t\frac{q+1}{2}$. We claim $\frac{q-1}{a}\nmid(t+1)$, otherwise $t=r\frac{q-1}{a}-1$ for $1\le r\le a$ since $0\le j,l\le q-2$. But $qj+l=(r\frac{q-1}{a}-1)\frac{q+1}{2}=(r\frac{q-1}{2a}-1)q+r\frac{q-1}{2a}+\frac{q-1}{2}$, then $(a+1)m\le l=r\frac{q-1}{2a}+\frac{q-1}{2}\le q-1$, which is a contradiction. Thus

$$\begin{aligned}&\sum_{i=1}^n v_i^{q+1}a_i^{qj+l}\\&=\frac{q+1}{2}\sum_{i=1}^{\frac{q-1}{a}}\omega^{ai(q+1)}(\omega^{a(2i+1)(qj+l)}+\omega^{a(2i+2)(qj+l)})\\&=\frac{q+1}{2}\omega^{at(q+1)}\sum_{i=1}^{\frac{q-1}{a}}\omega^{ai(q+1)(t+1)}+\frac{q+1}{2}\omega^{at\frac{q+1}{2}}\sum_{i=1}^{\frac{q-1}{a}}\omega^{ai(q+1)(t+1)}\\&=0.\end{aligned}$$

Then by Lemma 3.1, $\mathrm{GRS}_k(\mathbf{a},\mathbf{v})\subseteq\mathrm{GRS}_k(\mathbf{a},\mathbf{v})^{\perp H}$. ■

Theorem 3.3. *Let* q *be an odd prime power with the form* $2am+1$*, then there exists a* q*-ary* $[[\frac{q^2-1}{a},\frac{q^2-1}{a}-2d+2,d]]$*-quantum MDS code, where* $2\le d\le(a+1)m+1$*.*

Proof: The proof is a straightforward application of Corollary 2.2 and Theorem 3.2. ■

As an immediate consequence of Theorem 3.3, we have the following corollary by taking $a=1$.

Corollary 3.4. *Let* q *be an odd prime power, then there exists a* q*-ary* $[[q^2-1,q^2-2d+1,d]]$*-quantum MDS code, where* $2\le d\le q$*.*

Remark 3.5. *In [11], [21], the authors showed that there exists a* q*-ary* $[[q^2-1,q^2-2d+1,d]]$*-quantum MDS code, where* q *is an odd prime power and* $2\le d\le q-1$*. Obviously, our result has larger minimum distance.*

B. New Quantum MDS Codes of Length $\frac{q^2-1}{2a}-q+1$

In this subsection, we will construct quantum MDS codes of length $\frac{q^2-1}{2a}-q+1$. For our purpose, we need the following lemma.

Lemma 3.6. [15] Let A be an $(n-1)\times n$ matrix of rank $n-1$ over $\mathbb{F}_{q^2}$. Then the equation $Ax=0$ has a nonzero solution in $\mathbb{F}_q$ if and only if $A^{(q)}$ and A are row equivalent, where $A^{(q)}$ is obtained from A by raising every entry to its q-th power.

Theorem 3.7. *Let q be an odd prime power with the form $2am-1$ and $n=\frac{q^2-1}{2a}-q+1$, then there exist $\mathbf{a}\in\mathbb{F}_{\mathbf{q^2}}^{\mathbf{n}}$ and $\mathbf{v}\in(\mathbb{F}_{\mathbf{q^2}}^{*})^{\mathbf{n}}$ such that $\mathrm{GRS}_k(\mathbf{a},\mathbf{v})\subseteq\mathrm{GRS}_k(\mathbf{a},\mathbf{v})^{\perp H}$ for $1\le k\le(a+1)m-3$.*

Proof: Let ω be a fixed primitive element of $\mathbb{F}_{q^2}$. We also let A be an $(m-2)\times(m-1)$ matrix with $A_{ij}=\omega^{2j(m-3+(q-1)(i-1))}$ for $1\le i\le m-2,\ 1\le j\le m-1$.

Since $(m-3+(q-1)(i-1))q\equiv(m-3+(q-1)(m-i-2)) \pmod{q^2-1}$ for $1\le i\le m-2$, then $A^{(q)}$ and A are row equivalent. By Lemma 3.6, there exists $\mathbf{c}\in\mathbb{F}_q^{m-1}$ such that $A\cdot\mathbf{c}^t=0$. Note that by deleting any one column of matrix A, the remaining matrix is a Vandermonde matrix, hence all coordinates of $\mathbf{c}$ are nonzero. So we can represent $\mathbf{c}$ as $\mathbf{c}=(\omega^{a_1(q+1)},\cdots,\omega^{a_{m-1}(q+1)})$.

Now let $\mathbf{a}=(\omega^{2a},\omega^{4a},\cdots,\omega^{q+1-2a},\omega^{q+1+2a},\cdots,\omega^{2q+2-2a},\cdots,\omega^{q^2-q-2+2a},\cdots,\omega^{q^2-1-2a})\in\mathbb{F}_{q^2}^n$ and $\mathbf{v}=(\omega^{a_1},\cdots,\omega^{a_{m-1}},\omega^{a_1-(m-3)},\cdots,\omega^{a_{m-1}-(m-3)},\cdots,\omega^{a_1-(m-3)(q-2)},\cdots,\omega^{a_{m-1}-(m-3)(q-2)})\in(\mathbb{F}_{q^2}^*)^n$. Then for $0\le j,l\le k-1\le(a+1)m-4$, we have

$$\begin{aligned}&\sum_{i=1}^{n}v_i^{q+1}a_i^{qj+l}\\ &=\sum_{i=1}^{m-1}\omega^{a_i(q+1)+2ai(qj+l)}\sum_{s=0}^{q-2}\omega^{(q+1)(qj+l-m+3)s}.\end{aligned}$$

Note that

$$\sum_{s=0}^{q-2}\omega^{(q+1)(qj+l-m+3)s}=\begin{cases}0; & \text{if } (q-1)\nmid(qj+l-m+3),\\ q-1; & \text{if } (q-1)|(qj+l-m+3).\end{cases}$$

Assume $qj+l-m+3=t(q-1)$, we claim that $t\not\equiv m-2,m-1 \pmod m$. Otherwise, if $t\equiv m-2 \pmod m$, let $t=rm+m-2$, then $0\le r\le a$. If $r\le a-1$, then $qj+l=t(q-1)+m-3=(mr+m-3)q+(q-mr-1)=(mr+m-3)q+(2a-r)m-2$ and $(2a-r)m-2>(a+1)m-4$ which is a contradiction. If $r=a$, then $qj+l=t(q-1)+m-3=(am+m-3)q+(am-2)$ and $am+m-3>(a+1)m-4$, which is also a contradiction. Similarly, $t\not\equiv m-1 \pmod m$. Hence $qj+l \pmod{\frac{q^2-1}{2a}}\in\{t(q-1)+m-3|0\le t\le m-3\}$. Thus

$$\begin{aligned}&\sum_{i=1}^{n}v_i^{q+1}a_i^{qj+l}\\ &=(q-1)\sum_{i=1}^{m-1}\omega^{a_i(q+1)+2ai(qj+l)}\\ &=0,\end{aligned}$$

where the last equation is from the definition of $\mathbf{c}$. Then by Lemma 3.1, $\mathrm{GRS}_k(\mathbf{a},\mathbf{v})\subseteq\mathrm{GRS}_k(\mathbf{a},\mathbf{v})^{\perp H}$. ∎

Theorem 3.8. *Let q be an odd prime power with the form $2am-1$, then there exists a q-ary $[[\frac{q^2-1}{2a}-q+1,\frac{q^2-1}{2a}-q-2d+3,d]]$-quantum MDS code, where $2\le d\le(a+1)m-2$.*

Proof: The proof is a straightforward application of Corollary 2.2 and Theorem 3.7. ∎

In particular, taking $a=1$, we obtain the following corollary.

Corollary 3.9. *Let $q\ge5$ be an odd prime power, then there exists a q-ary $[[\frac{q^2-1}{2}-q+1,\frac{q^2-1}{2}-q-2d+3,d]]$-quantum MDS code, where $2\le d\le q-1$.*

C. New Quantum MDS Codes of Length $\frac{q^2-1}{2a+1}-q+1$

In this subsection, we consider quantum MDS codes of length $\frac{q^2-1}{2a+1}-q+1$.

Theorem 3.10. *Let q be an odd prime power with the form $(2a+1)m-1$ and $n=\frac{q^2-1}{2a+1}-q+1$, then there exist $\mathbf{a}\in\mathbb{F}_{\mathbf{q^2}}^{\mathbf{n}}$ and $\mathbf{v}\in(\mathbb{F}_{\mathbf{q^2}}^*)^{\mathbf{n}}$ such that $\mathrm{GRS}_k(\mathbf{a},\mathbf{v})\subseteq\mathrm{GRS}_k(\mathbf{a},\mathbf{v})^{\perp H}$ for $1\le k\le(a+1)m-2$.*

Proof: Let ω be a fixed primitive element of $\mathbb{F}_{q^2}$. We also let A be an $(m-2)\times(m-1)$ matrix with $A_{ij}=\omega^{(i(q-1)-1)j}$ for $1\le i\le m-2,\ 1\le j\le m-1$.

Since $(i(q-1)-1)q\equiv((q-i)(q-1)-1)\pmod{q^2-1}$ for $1\le i\le q-1$, then $A^{(q)}$ and A are row equivalent. By Lemma 3.6, there exists $\mathbf{c}\in\mathbb{F}_q^{m-1}$ such that $A\cdot\mathbf{c}^t=0$. Since by deleting any one column of matrix A, the remaining matrix is a Vandermonde matrix, then all coordinates of $\mathbf{c}$ are nonzero. Hence we can represent $\mathbf{c}$ as $\mathbf{c}=(\omega^{a_1(q+1)},\cdots,\omega^{a_{m-1}(q+1)})$.

Now let $\mathbf{a}=(\omega^{2a+1},\omega^{2(2a+1)},\cdots,\omega^{q-2a},\omega^{q+2a+2},\cdots,\omega^{2q+1-2a},\cdots,\omega^{q^2-q-1+2a},\cdots,\omega^{q^2-2-2a})\in\mathbb{F}_{q^2}^n$ and $\mathbf{v}=(\omega^{a_1},\cdots,\omega^{a_{m-1}},\omega^{a_1+1},\cdots,\omega^{a_{m-1}+1},\cdots,\omega^{a_1+q-2},\cdots,\omega^{a_{m-1}+q-2})\in(\mathbb{F}_{q^2}^*)^n$. Then for $0\le j,l\le k-1\le(a+1)m-3$, we have

$$\begin{aligned}&\sum_{i=1}^{n}v_i^{q+1}a_i^{qj+l}\\&=\sum_{i=1}^{m-1}\omega^{a_i(q+1)+i(qj+l)}\sum_{s=0}^{q-2}\omega^{(q+1)(qj+l+1)s}.\end{aligned}$$

Note that

$$\sum_{s=0}^{q-2}\omega^{(q+1)(qj+l+1)s}=\begin{cases}0; & \text{if } (q-1)\nmid(qj+l+1),\\ q-1; & \text{if } (q-1)|(qj+l+1).\end{cases}$$

Assume $qj+l+1=t(q-1)$, then $t\not\equiv 0,m-1\pmod m$. Otherwise, if $t\equiv 0\pmod m$, let $t=rm$. Then $qj+l=t(q-1)-1=(rm-1)q+(2a+1-r)m-2$ and $\min\{rm-1,(2a+1-r)m-2\}>(a+1)m-3$, which is a contradiction. Similarly, $t\not\equiv m-1\pmod m$. Thus

$$\begin{aligned}&\sum_{i=1}^{n}v_i^{q+1}a_i^{qj+l}\\&=(q-1)\sum_{i=1}^{m-1}\omega^{a_i(q+1)+i(qj+l)}\\&=0,\end{aligned}$$

where the last equation is from the definition of $\mathbf{c}$. Then by Lemma 3.1, $\mathrm{GRS}_k(\mathbf{a},\mathbf{v})\subseteq\mathrm{GRS}_k(\mathbf{a},\mathbf{v})^{\perp H}$. ■

Theorem 3.11. *Let q be an odd prime power with the form $(2a+1)m-1$, then there exists a q-ary $[[\frac{q^2-1}{2a+1}-q+1,\frac{q^2-1}{2a+1}-q-2d+3,d]]$-quantum MDS code, where $2\le d\le(a+1)m-1$.*

Proof: The proof is a straightforward application of Corollary 2.2 and Theorem 3.10. ■

In particular, taking $a=0$, we obtain the following corollary.

Corollary 3.12. *Let q be an odd prime power, then there exists a q-ary $[[q^2-q,q^2-q-2d+2,d]]$-quantum MDS code, where $2\le d\le q$.*

IV. New Quantum Codes from Matrix-Product Codes

Let $A=(a_{ij})$ be an $s\times s$ matrix with entries in $\mathbb{F}_{q^2}$, we define $A^{(q)}=(a_{ij}^q)$. Then we have the following result.

Lemma 4.1. *Let $A=(a_{ij})$ be a nonsingular $s\times s$ matrix such that $A^{(q)}$ is also nonsingular. Suppose there exist linear codes C_i such that $C_i^{\perp H}\subseteq C_i$ for $i=1,2,\cdots,s$. Then*

$$([C_1,C_2,\cdots,C_s]\cdot A)^{\perp H}\subseteq[C_1,C_2,\cdots,C_s]\cdot[(A^{(q)})^{-1}]^t.$$

Proof: By Theorem 2.4, we have

$$\begin{aligned}([C_1, C_2, \cdots, C_s] \cdot A)^{\perp H} &= ([C_1^q, C_2^q, \cdots, C_s^q] \cdot A^{(q)})^{\perp E} \\ &= [(C_1^q)^{\perp E}, (C_2^q)^{\perp E}, \cdots, (C_s^q)^{\perp E}] \cdot [(A^{(q)})^{-1}]^t \\ &= [C_1^{\perp H}, C_2^{\perp H}, \cdots, C_s^{\perp H}] \cdot [(A^{(q)})^{-1}]^t \\ &\subseteq [C_1, C_2, \cdots, C_s] \cdot [(A^{(q)})^{-1}]^t.\end{aligned}$$

■

Now we would like to use matrix-product codes to construct quantum codes.

Corollary 4.2. *Let $q = p^t$ be an odd prime power, where p is a prime number. Suppose C_1, C_2 are linear codes over $\mathbb{F}_{q^2}$ with parameters $[n, k_i, d_i]$ and $C_i^{\perp H} \subseteq C_i$, $i = 1, 2$. Then there exists a Hermitian dual containing $[2n, k_1 + k_2, \geq \min\{2d_1, d_2\}]$ code over $\mathbb{F}_{q^2}$.*

Proof: Take

$$A = \begin{pmatrix} 1 & 1 \\ 1 & p-1 \end{pmatrix},$$

then

$$[(A^{(q)})^{-1}]^t = \begin{pmatrix} \frac{p+1}{2} & \frac{p+1}{2} \\ \frac{p+1}{2} & \frac{p-1}{2} \end{pmatrix}.$$

By Lemma 4.1, we have

$$\begin{aligned}([C_1, C_2] \cdot A)^{\perp H} &\subseteq [C_1, C_2] \cdot [(A^{(q)})^{-1}]^t \\ &= [C_1, C_2] \cdot A.\end{aligned}$$

Applying Theorem 2.3, $[C_1, C_2] \cdot A$ is a Hermitian dual containing $[2n, k_1 + k_2, \geq \min\{2d_1, d_2\}]$ code. ■

The following result can be found in [11], [14], [15].

Theorem 4.3. *Let q be an odd prime power, then*

1) *there exists a q^2-ary Hermitian dual containing $[q^2 + 1, q^2 + 2 - d, d]$ code for $1 \leq d \leq q + 1$;*
2) *there exists a q^2-ary Hermitian dual containing $[q^2, q^2 + 1 - d, d]$ code for $2 \leq d \leq q$.*

By combing Theorems 4.3, 3.2 and Corollary 4.2, we can immediately get the following lemma.

Lemma 4.4. *Let q be an odd prime power, then*

1) *there exists a q^2-ary Hermitian dual containing $[2q^2 + 2, 2q^2 + 4 - d - \frac{d}{2}, d]$ code, where $2 \leq d \leq q + 1$ is even;*
2) *there exists a q^2-ary Hermitian dual containing $[2q^2 + 2, 2q^2 + 3 - d - \frac{d-1}{2}, d]$ code, where $2 \leq d \leq q + 1$ is odd;*
3) *there exists a q^2-ary Hermitian dual containing $[2q^2, 2q^2 + 2 - d - \frac{d}{2}, d]$ code, where $2 \leq d \leq q$ is even;*
4) *there exists a q^2-ary Hermitian dual containing $[2q^2, 2q^2 + 1 - d - \frac{d-1}{2}, d]$ code, where $2 \leq d \leq q$ is odd;*
5) *there exists a q^2-ary Hermitian dual containing $[2q^2 - 2, 2q^2 - d - \frac{d}{2}, d]$ code, where $2 \leq d \leq q$ is even;*
6) *there exists a q^2-ary Hermitian dual containing $[2q^2 - 2, 2q^2 - 1 - d - \frac{d-1}{2}, d]$ code, where $2 \leq d \leq q$ is odd.*

Then by the Hermitian construction and Lemma 4.4, we have the following theorem.

Theorem 4.5. *Let q be an odd prime power, then*

1) *there exists a q-ary $[[2q^2 + 2, 2q^2 + 6 - 3d, \geq d]]$ quantum code, where $2 \leq d \leq q + 1$ is even;*
2) *there exists a q-ary $[[2q^2 + 2, 2q^2 + 5 - 3d, \geq d]]$ quantum code, where $2 \leq d \leq q + 1$ is odd;*
3) *there exists a q-ary $[[2q^2, 2q^2 + 4 - 3d, \geq d]]$ quantum code, where $2 \leq d \leq q$ is even;*
4) *there exists a q-ary $[[2q^2, 2q^2 + 3 - 3d, \geq d]]$ quantum code, where $2 \leq d \leq q$ is odd;*
5) *there exists a q-ary $[[2q^2 - 2, 2q^2 + 2 - 3d, \geq d]]$ quantum code, where $2 \leq d \leq q$ is even;*
6) *there exists a q-ary $[[2q^2 - 2, 2q^2 + 1 - 3d, \geq d]]$ quantum code, where $2 \leq d \leq q$ is odd.*

In Table I, we list some quantum codes obtained from Theorem 4.5. The table shows that our quantum codes have better parameters than the previous quantum codes available.

TABLE I
QUANTUM CODES COMPARISON

new quantum codes	quantum codes from [9]
$[[20,14,\geq 3]]_3$	$[[20,12,3]]_3$
$[[48,28,\geq 8]]_5$	$[[48,26,8]]_5$
$[[52,44,\geq 4]]_5$	$[[52,42,4]]_5$
$[[52,40,\geq 5]]_5$	$[[52,38,5]]_5$
$[[96,64,\geq 12]]_7$	$[[96,62,12]]_7$
$[[100,92,\geq 4]]_7$	$[[100,92,3]]_7$
$[[164,152,\geq 5]]_9$	$[[164,150,5]]_9$
$[[164,156,\geq 4]]_9$	$[[164,154,4]]_9$

REFERENCES

[1] S. A. Aly, A. Klappenecker, and P. K. Sarvepalli, "On quantum and classical BCH codes," *IEEE Trans. Inform. Theory*, vol. 53, no. 3, pp. 1183–1188, 2007.

[2] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 3065–3072, 2001.

[3] J. Bierbrauer and Y. Edel, "Quantum twisted codes," *J. Combin. Des.*, vol. 8, no. 3, pp. 174–188, 2000.

[4] T. Blackmore and G. H. Norton, "Matrix-product codes over $\mathbb{F}_q$," *Appl. Algebra Engrg. Comm. Comput.*, vol. 12, no. 6, pp. 477–500, 2001.

[5] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.*, vol. 78, no. 3, pp. 405–408, 1997.

[6] ——, "Quantum error correction via codes over $\mathrm{GF}(4)$," *IEEE Trans. Inform. Theory*, vol. 44, no. 4, pp. 1369–1387, 1998.

[7] B. Chen, S. Ling, and G. Zhang, "Application of constacyclic codes to quantum MDS codes," *IEEE Trans. Inform. Theory*, vol. 61, no. 3, pp. 1474–1484, 2015.

[8] H. Chen, S. Ling, and C. Xing, "Quantum codes from concatenated algebraic-geometric codes," *IEEE Trans. Inform. Theory*, vol. 51, no. 8, pp. 2915–2920, 2005.

[9] Y. Edel, "Some good quantum twisted codes," Online available at https://www.mathi.uni-heidelberg.de/$\sim$yves/Matritzen/QTBCH/QTBCHIndex.html.

[10] C. Galindo, F. Hernando, and D. Ruano, "New quantum codes from evaluation and matrix-product codes," arXiv:1406.0650.

[11] M. Grassl, T. Beth, and M. Roetteler, "On optimal quantum codes," *Int. J. Quantum Inf.*, vol. 2, no. 01, pp. 55–64, 2004.

[12] M. Grassl, M. Rotteler, and T. Beth, "On quantum MDS codes," in *Proc. Int. Symp. Inf. Theory, Chicago, June*, 2004, p. 355.

[13] F. Hernando, K. Lally, and D. Ruano, "Construction and decoding of matrix-product codes from nested codes," *Appl. Algebra Engrg. Comm. Comput.*, vol. 20, no. 5-6, pp. 497–507, 2009.

[14] L. Jin, S. Ling, J. Luo, and C. Xing, "Application of classical Hermitian self-orthogonal MDS codes to quantum MDS codes," *IEEE Trans. Inform. Theory*, vol. 56, no. 9, pp. 4735–4740, 2010.

[15] L. Jin and C. Xing, "A construction of new quantum MDS codes," *IEEE Trans. Inform. Theory*, vol. 60, no. 5, pp. 2921–2925, 2014.

[16] X. Kai, S. Zhu, and P. Li, "Constacyclic codes and some new quantum MDS codes," *IEEE Trans. Inform. Theory*, vol. 60, no. 4, pp. 2080–2086, 2014.

[17] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, "Nonbinary stabilizer codes over finite fields," *IEEE Trans. Inform. Theory*, vol. 52, no. 11, pp. 4892–4914, 2006.

[18] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," *Phys. Rev. A (3)*, vol. 55, no. 2, pp. 900–911, 1997.

[19] G. G. La Guardia, "New quantum MDS codes," *IEEE Trans. Inform. Theory*, vol. 57, no. 8, pp. 5551–5554, 2011.

[20] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek, "Perfect quantum error correcting code," *Phys. Rev. Lett.*, vol. 77, no. 1, p. 198, 1996.

[21] Z. Li, L. Xing, and X. Wang, "Quantum generalized Reed-Solomon codes: unified framework for quantum maximum-distance-separable codes," *Phys. Rev. A (3)*, vol. 77, no. 1, pp. 012 308, 4, 2008.

[22] E. M. Rains, "Nonbinary quantum codes," *IEEE Trans. Inform. Theory*, vol. 45, no. 6, pp. 1827–1832, 1999.

[23] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A*, vol. 52, no. 4, p. R2493, 1995.

[24] A. Steane, "Multiple-particle interference and quantum error correction," *Proc. Roy. Soc. London Ser. A*, vol. 452, no. 1954, pp. 2551–2577, 1996.

[25] A. M. Steane, "Enlargement of Calderbank-Shor-Steane quantum codes," *IEEE Trans. Inform. Theory*, vol. 45, no. 7, pp. 2492–2495, 1999.